November 17, 2020

Selecting the Right Identity Provider for Kubernetes: a Comparative Survey

SUSE

Welcome

Cameron Seader

Cameron Seader is a Technology Strategist at SUSE, working with the most strategic opportunities and premium customers around open source technologies like Kubernetes, Ceph, Cloud Foundry, and more. With over 20 years of experience in data center systems to application platforms as a domain expert in these technologies. During the OpenStack era he was a domain expert and creator of the OpenStack Cloud Appliance. He has led teams that meet and exceed business outcomes. Participates in the CNCF Security SIG, openSUSE community, and others. He's been a speaker at many industry and partner events over the years. Exploring the mountains of Idaho, boating in the mountain lakes, and photographing the landscape is some of his favorite pastime. Join the #PowerOfMany #SUSE

Technology Strategist
Twitter @camseader
https://www.linkedin.com/in/cseader

Who do you trust in this ever-evolving web of Identities?

01 Let's talk about Identities

Where, Why, how, and things.

02 IdP for K8s

What Identity Providers are available and what are the common markers of interest.

03 What's best for me?

Common marker comparison and how we conclude on the right IdP for me.

Let's talk about Identities

Identity Evolution

From the invention of the transistor to billions of them in the palm of your hand.

We are mostly creating our own problems with unique solutions.

We are becoming perfectionists by way of community technologists.

AuthN and AuthZ strategies

AuthN

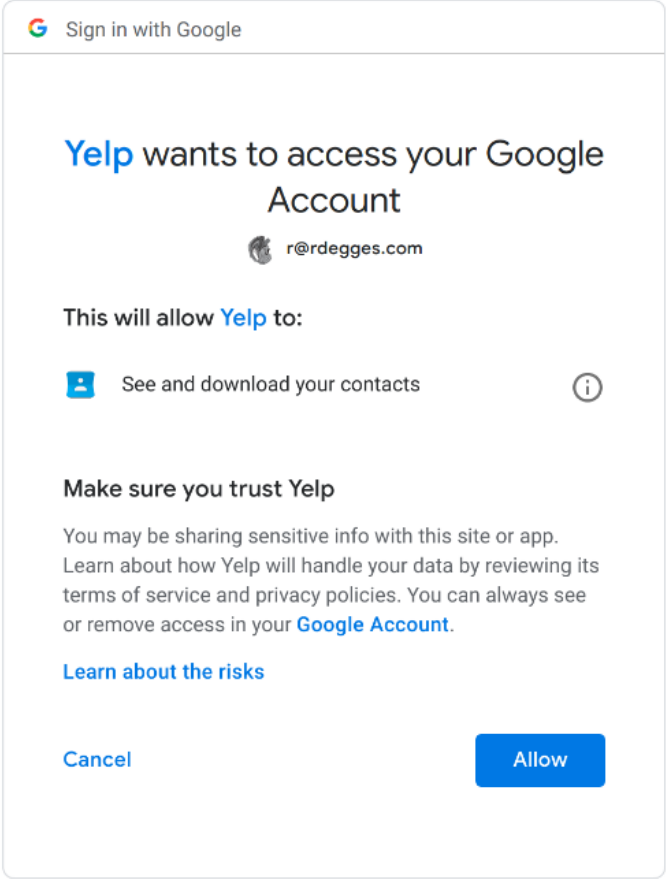
- X509 client certificates
- Tokens:
  - Static token file
  - OpenID Connect tokens
  - Webhook tokens
  - Bootstrap tokens
  - Service account tokens
- Static password
- Anonymous requests

AuthZ

- RBAC
- Webhook
- Node Authorizer

SAML vs OAuth vs OIDC

Use Cases	
Access to applications from a portal	SAML, OAuth2+OpenID Connect
Centralized identity source (IdP)	SAML, OAuth2+OpenID Connect
SSO for Enterprise	SAML, OAuth2+OpenID Connect
Provide access to a partner or customer portal	SAML, OAuth2+OpenID Connect
Mobile device use	OAuth2+OpenID Connect
Providing access to resources	OAuth2+OpenID Connect



OIDC and OAuth to infinity, maybe

We have AuthN and AuthZ seemingly figured out

BUT…

- Its complex
- Developers don’t want to care about managing tokens and crypto
- Authenticate users and check their access
- Client libraries are important

The Kubernetes Way

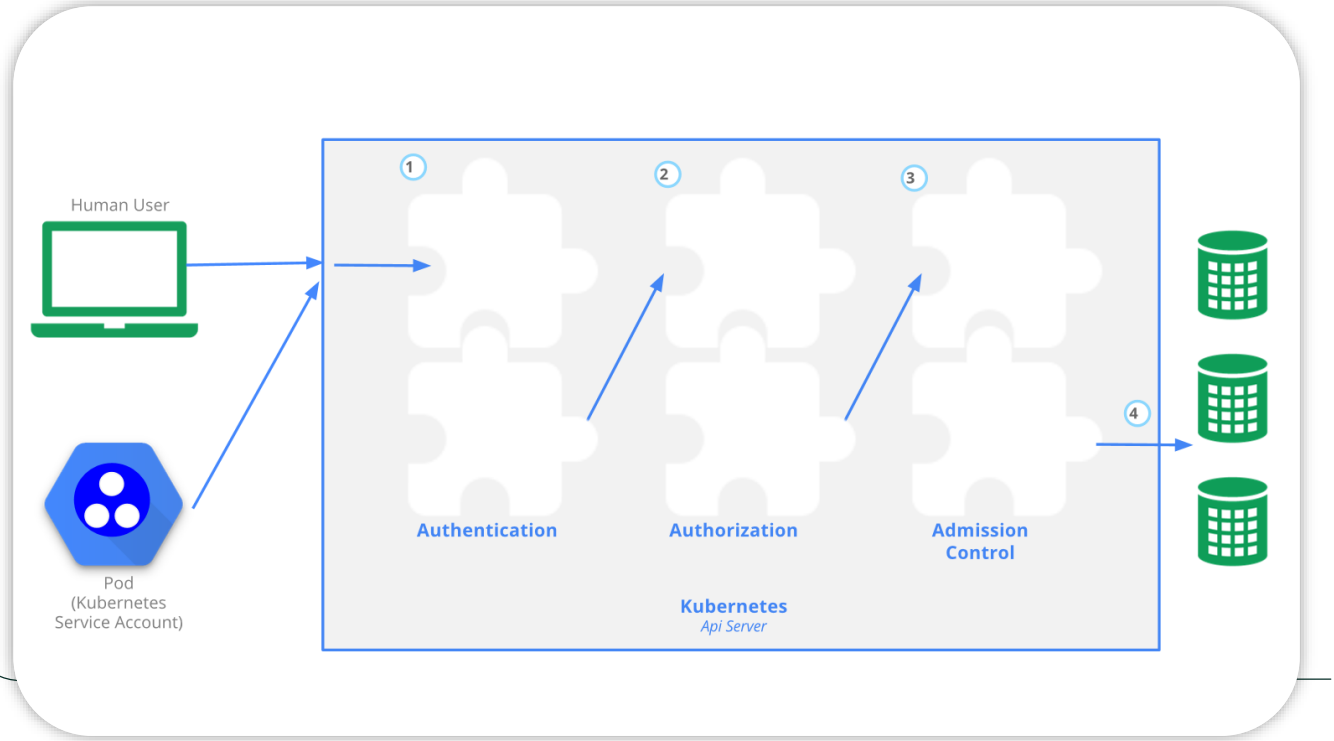
Plugins

http Basic Authentication (Base64)

OpenID Connect

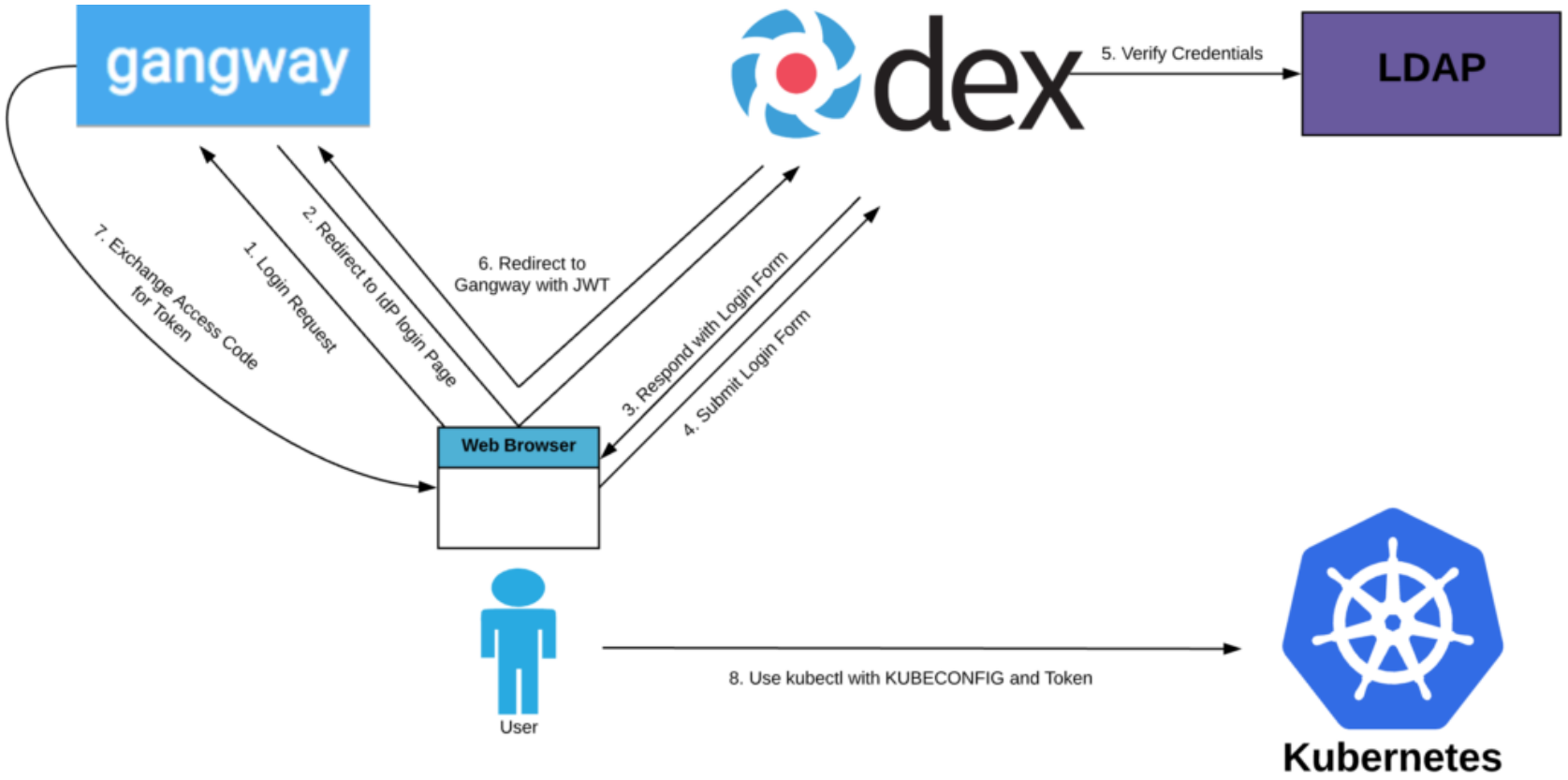
Token Auth (Static, Webhook)…

Let's count the ways.



IdP for K8s

Typical IdP Architecture (for K8s)



Do we still need LDAP in 2020?

Positive

Its been proven for ages and still used by the enterprise

Easy to migration to another IdP

Used as a base for unified SSO

You already have it somewhere?

Deployable on K8s

Negative

Declarative is not sufficient

Stateful, You better make a backup

No 2FA

Not usable as is

It doesn’t scale

- NoSQL to the rescue

Portals to another IdP

*dex

*UAA

OpenUnison

OIDC Clients

Stratos

Gangway

dex-k8s-authenticator

Tremolo Security's Kubectl-login

…. Your choice

The Outstanding in the Crowd
with open source street cred

Gluu

Our current goal is to be among the first vendors to support all new (essential) features of OAuth. This requires a lot of innovation, and so far I think Gluu's community-driven approach, and focus on easy deployment via Linux packages, and K8s support, has delivered more OAuth features and a larger ecosystem of early adoption.

KeyCloak

Keycloak is an Open Source Identity and Access Management solution for modern Applications and Services.

OpenUnison

OpenUnison combines the common identity management functions needed by most applications including, SSO, User Provisioning (with Workflows), Federation, Web Services. OpenUnison can run on any J2EE container (such as Tomcat or JBoss).

OpenIAM

In 2008, we started OpenIAM with the mission of making the business of managing identities effortless using an innovative approach -- a model which leverages an agile collaboration between our customers and our exceptionally talented engineering team. All of our products are designed in-house and use the latest technology, allowing customers the freedom to adopt as much or as little of the solution based on their current and future needs.

Common Markers of Interest

Marker	
Identity Federation	Linking of identities and attributes across IdP's
Open Source	Level of Open Source software
Protocol Support	AuthN, AuthZ protocol support available
Second Factor Auth	Extra layer of security protocols available
User Management	Tools to support the management of Users
Automated Client Registration	Client-side application to support self service
Backend Support	Support for backend types such as LDAP, Database, etc
Language	The language it was developed in primarily
Architecture	Native library support for developers or just connectors
Developer Community	Is the community active developing / contributing
Helm chart / Easy K8s	Easily deployable on K8s

What’s best for me?

Let’s Compare

Marker	KeyCloak	OpenUnison	Gluu	OpenIAM
Identity Federation	Yes	Yes	Yes	Yes
Open Source	Yes, with extras for enterprise	100%	100%	Yes, with extras for enterprise
Protocol Support	OIDC/OAuth2/SAML2	SAML2/OIDC/SAML2	OIDC/OAuth2/SAML2/UMA/OPA /CAS	OIDC/OAuth2/SAML2
Second Factor Auth	OTP, U2F, TOTP	OTP, FIDO2 U2F, TOTP	OTP, FIDO2 U2F, TOTP	OTP, FIDO2 U2F (EE), TOTP
User Management	Web Interface, API, CLI	Web Interface, API	Web Interface, API, Mobile App	Web Interface, API
Automated Client Registration	Yes	Yes	Yes	Yes
Backend Support	LDAP, AD, others possible	LDAP, AD, MongoDB, other DBs, K8s API	AD, LDAP, Couchbase, K8s API	AD, LDAP
Language	Java	Java	Java	Java
Developer Community	Active, No Roadmap	Active	Active, Current Roadmap	Can’t find info
Architecture	Some client libraries	Client libraries, support for many languages	Client libraries, support for many languages	Some client libraries
Helm chart / Easy K8s	Yes	Yes	Yes	Yes, (EE)

OpenID Certified

Certified OpenID Provider Servers and Services

- Gluu Server 4.x, Keycloak – old version

Certified Financial-grade API (FAPI)

- Gluu Server 4.2

Certified Financial-grade API Client Initiated Back channel Authentication Profile (FAPI-CIBA)

- Gluu Server 4.2

But I can just use dex, or UAA

Sure you can…

There are ways with dex that are great

- Use a client application such as gangway or dex-k8s-authenticator
- Not enterprise scope

UAA is User Account and Authentication

- More well known to the Cloud Foundry Community
- Works similarly to dex
- Still need a client application
- It does have an OpenID Certification

Conclusion

Outstanding in the crowd

Certified

Enterprise Ready

Tight integration

Administrator Tools

Covers the whole protocol base

continuous improvement (Oauth 3?)

For more information, contact SUSE at:

+1 800 796 3700 (U.S./Canada)

+49 (0)911-740 53-0 (Worldwide)

SUSE

Maxfeldstrasse

90409 Nuremberg

www.suse.com